Assumption Busters Workshop – Trust Anchors

Background: the U.S. Federal Cyber Research Community is conducting a series of four workshops designed to examine key assumptions that underlie current security architectures in cyberspace. These "Assumption Busters" meetings are designed to create the environment for the development of novel solutions that are based on a fundamentally different understanding of the problem and creates a stronger basis for moving forward on well-founded assumptions.

In the next few months, we will assess the problem for each assumption as well as any potential weaknesses that transcend the four categories: defense-in-depth, trust anchors, data dispersion, and malicious actors.

Introduction: the second "Assumption Buster" workshop was held on 27 April 2011 at Fort Meade, Maryland to focus on the assumption that "trust anchors are invulnerable". Over 30 participants from academia, government, industry and the research community attended the day-long open discussion. The day was organized, first, around the specific issues of public key cryptography and trusted platform module issues, followed by a broader discussion about platforms and architectures. A final session broached the issue of defining trust within this security context. This paper identifies key themes that support or challenge the assumption. It then identifies near- and long-term directions for further research and exploration.

Assumption: Trust anchors are invulnerable.

Bottom Line: Clearly false, especially when one considers the word "invulnerable" to mean incapable of being wounded, hurt or damaged, and thereby rendered ineffective. But there are concepts for improving individual trust anchors and layering them in different ways to improve overall security. Trust anchors may actually attract more attention from attackers because of the high potential value associated with breaking them. One key source of vulnerability is that trust anchors are often thought of as an add-on capability in a system, vice developed as an integrated part of the system.

Ideas that Support the Assumption:

-- No one supported the absolute assumption, however, some of the critical assumptions that underlie our thinking about trust anchors are at risk, such as the strength of current public asymmetric key cryptography and the variance between how trusted platform modules ought to be built and implemented and how they actually are.

-- Participants did focus on improvements within individual trust anchors to make them less vulnerable and the prospects of layering to decrease the vulnerability of a system. Managing

trust anchors and the relationship between them is important, however, affecting human behavior in how they perceive and use trust anchors appear to be of tantamount importance. What constitutes trust, and how it relates to security, was a key focal point for discussion.

Ideas that Challenge the Assumption:

-- Participants focused on an improved understanding of what trust anchors actually do or do not do in the three different categories – public key, trusted platform modules, and system design – and some of the sources of vulnerability associated with them. They also focused on dependencies for successful operation and the human factors associated with them.

-- *Public key infrastructure*: Participants talked about the state of public key encryption, with some view that a new system is necessary. Government and industry value identity within a transaction very differently for their own purposes, as the former places great value on knowing identity while the latter cares more about legitimate transactions. Public certificate use in the commercial world has become narrower in light of that, with an emphasis on certificates, not domain names. Highly regulated industries like pharmaceuticals and research and education are implementing their own certificate programs but there is neither a transition to other industries nor a full understanding on how to create incentives to use them. There are some other boutique PKI systems under development that include the DNS SEC signed for system control. People who actually use public key certificates often do not know what they really mean in terms of risk, authority, and accountability. Finally, no matter how many certificates or security mechanisms are put in place, some individual users will not participate.

-- *Trusted Platform Modules:* Trusted platform modules, or TPMs, can exist in hardware or software – software TPMs are often anchored in hardware TPMs. They are thought to represent a root of trust for reporting and a root of trust for storage. Participants questioned the manner and extent to which trust and trustworthiness can be measured, and how often. TPMs are often built to defend against attack from outside the system, and gain their trustworthiness from their passive nature. But this prompts a number of other questions about vulnerability: if working with hardware TPMs, how can a trusted path be built between the user and the chip itself? How does an attack that emanates from inside the machine interact with or dupe the TPM. TPMs can detect what is going on, but has no ability to change or shut down functions. In essence, it is an overseer, not an enforcer.

-- *Computing Platforms and Architectures:* Within computing platform components – the operating system, the hypervisor or virtual machine monitor, the system firmware, and the CPU and chipset, there are multiple opportunities for security guarantees, including protection of security mechanisms, software and application measurement, and separation of data and processes. Vulnerabilities are created when the platform does not allow for the security functionality to perform in these roles, either because of design or implementation failures. Platforms may themselves carry malicious code or components that weaken or damage these

security guarantees, including those linked to PKI and TPM, Some vulnerability is created simply by the failure to use security functionality that is present. Sometimes, flawed integration with the rest of the system – such as where applications re-invent their own security mechanisms rather than using system ones – creates vulnerability. System improvements in other areas – such as energy efficiency – sometimes conflict with security goals. A strong debate emerged about the comparative value of security in hardware versus security in software.

-- *Human Factors:* Central to secure computing is the role of the user, regardless of the importance of use and the consequence of failure. Vulnerability is created where uninformed users fail to understand the security signals (e.g., the McAfee "green check"; warning notices) they receive, fail to act on them, or fail to consider the broader consequences of doing so (one may care less about the hack of a secondary e-mail, but not think about the potential implications on their banking or health data on the same computer). Even the most educated and conscientious user may be duped by deceptive link text or security indicator spoofing ("the locked lock"). Secure computing requires both trust in data and trust in people. Security is not trust – how would one set a sufficiency condition in security to establish human trust?

Areas for Further Research and Exploration:

-- **Understanding the Adversary**: For certain groups of adversaries – such as social hackers and the Russian crime networks – trust is essential, whether in terms of identity, credibility, and any assurance of capability and interest in certain operations. The "dark world" is developing its own reputation credentials and trust frameworks – what are they? How do they work? What levels of trust are required for which purposes?

-- **The Relationship of Trust Anchors to Trust Chains and/or Trust Frameworks**: More attention needs to be given to the ability to link or layer trust anchors within a broader framework. Which ones work best in tandem fashion? Where does the overall management of trust anchors take place? What is the state of development of trust frameworks that can be used widely?

-- **Human Factors and Trust Anchors**: How do we better educate people to understand and observe the rule sets created by trust anchors? How do we create the right incentives and disincentives for trust anchors to be used appropriately? What is the role of privacy in the trust anchors world?

-- **The Role of Partitioning**: Related to the above, people use computing systems for a multitude of applications, some casual, some very important. What is the role of system partitioning, and potential improvement to it, on both the system and the human side of secure computing? Partitioning, for example, might require that a user terminate all other applications in order to conduct a valuable banking application in order to ensure security of that transaction.

-- **The Economics of Trust Anchors**: How do we create the right incentives for trust anchors to be integrated from system design into new computing systems? There is a productive history of TPM that merits additional attention here, as well as the emergence of trust anchors in the mobile world.

-- **Historical Trade Spaces for Trust Anchors**: Understanding the assumptions made during the establishment of certain trust anchors – such as those about processing speeds, storage costs and others – could help identify alternate options in thinking about how to modify those trust anchors. This could be a graduate student challenge.

-- **The Search for a Place to Stand**: While many options exist to improve security on commodity computing platforms, more attention needs to be given to how and from where on the platform this is best done. Almost every modality has a comparative strength and weakness from which to manage platform security.

-- **Role of Government and Industry: Areas for Cooperation:** Finally, as in the other "Assumption Buster" workshops, there are areas of both converging and diverging interests between government and industry on these topics. What are the most promising areas of convergent interest? Industry groups have formed to discuss a broad set of topics ranging from trust in other endeavors (e.g. medicine, law) and how to improve trust in data. How do we incorporate government knowledge of more sophisticated threats and opportunities into this dialogue?